PRIVACY INVASION IN THE DIGITAL SPHERE: AN ANALYTICAL STUDY OF INDIAN LEGAL FRAMEWORK AND ETHICAL CONSIDERATIONS CONCERNING ONLINE PLATFORMS

A

SYNOPSIS

(THESIS PROPOSAL)

SUBMITTED TO

THE ICFAI University Dehradun

IN PARTIAL FULFILLMENT OF THE REQUIREMENT

FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY (Ph.D.)

IN

LAW

BY

ANUSHMI JAIN

(Enrollment No: RSILS200053)

Under the Supervision of

Dr. Susanta Kumar Shandangi

Associate Professor

ICFAI Law School

The ICFAI University, Dehradun

The ICFAI University, Dehradun

Candidate's Declaration

I, **Anushmi Jain**, declare that the synopsis entitled, **'Privacy Invasion in the Digital Sphere: An Analytical Study of Indian Legal Framework and Ethical Considerations concerning Online Platforms'** being submitted in the partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in Law under ICFAI Law School, The ICFAI University, Dehradun during the academic year 2023-24.

It is the work that is expected to carried out under the supervision of Dr. Susanta Kumar Shadangi It is further declared that the synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

Anushmi

Signature **Date:** 20/05/2024

Candidate's Name: Anushmi Jain

The ICFAI University, Dehradun

CERTIFICATE

This is to certify that the thesis entitled, **'Privacy Invasion in the Digital Sphere: An Analytical Study of Indian Legal Framework and Ethical Considerations concerning Online Platforms'** is an original piece of work done by ***Anushmi Jain*** under my supervision being submitted in the partial fulfilment of the requirement for the award of the degree of Doctor of Philosophy in Law under ICFAI Law School, The ICFAI University, Dehradun during the academic year 2023-24.

Further, it is certified that the synopsis is within the plagiarism limit and a copy of the same is attached as per the University norms.

Signature of the Supervisor in full

Name in Capital Letters DR. SUSANTA KUMAR SHADANGI

Designation & Address ASSOCIATE PROFESSOR
ICFAI UNIVERSITY
DEHRADUN

ABSTRACT

Privacy, an ever-evolving concept, has gained importance over time, aligning with the growing expectation of people seeking to protect their personal matters from unwarranted intrusions. Although the Constitution of India does not explicitly mention or recognise the 'right to privacy', judicial interpretations have enshrined it as a fundamental right, empowering individuals against unwarranted intrusions. Recognized globally as a human right, privacy underpins crucial principles such as human dignity, freedom of association, freedom of speech, etc. The importance of privacy has surged with advancements in information technology, which have dramatically increased data generation and potential for misuse. Social media, while connecting people, poses significant privacy risks due to its potential for misuse and unrestricted access by various entities. The Supreme Court of India in 2017, recognized privacy as a fundamental right, highlighting the loopholes and inadequacies in existing regulations and prompting the need for comprehensive privacy legislation. Despite multiple rejections, India enacted the 'Digital Personal Data Protection Act, 2023' (DPDPA), aiming to regulate data processing and grant citizens control over their information. However, the Act has notable deficiencies, including broad exemptions for government entities, potential loopholes, and concerns about legitimate uses of data without explicit consent. These issues could lead to unauthorized use and exploitation of personal data, compromising the privacy of individuals. Additionally, the Act's provisions regarding publicly available data raise further concerns about user privacy on online platforms. While the DPDPA marks progress in India's data protection efforts, it also underscores the ongoing challenges in safeguarding online privacy.

Keywords:

Privacy, Fundamental Right,, Information Technology, Social Media, Data Protection, Digital Personal Data Protection Act, Data Privacy, Online Privacy, Human Rights.

TABLE OF CONTENTS

1	Introduction	1
2	Research Questions	3
3.	Literature Review	3
4.	Research Gap	12
5.	Research Objectives	13
6.	Research Hypothesis	13
7.	Research Methodology	14
8.	Scope & Limitations of the Study	14
9.	Proposed Chapterisation	14
10.	Month-wise Plan of the Work	18
	Bibliography	19
	Plagiarism Certificate	

1. Introduction:

Privacy is an evolving concept that continues to gain importance over time, accompanied by people's expectations to preserve the same. Although the Constitution of India doesn't explicitly state the 'right to privacy', the judiciary has established it as a fundamental right through judicial interpretation, commonly referred to as the 'right to be left alone.[1]' This right empowers individuals to seek protection from unwarranted intrusions, ensuring that their personal matters cannot be encroached upon by others without a valid legal justification.

The 'right to privacy' is considered to be a human right that has been recognized in several International Conventions, for instance, 'UN Declaration of Human Rights', the ; International Covenant on Civil and Political Rights' and several other international as well as regional treaties Privacy serves as a foundation for essential principles like human dignity, freedom of association, and freedom of speech, etc. In the contemporary era, apparently, it has become a significant concern within the realm of human rights.

Ensuring respect for and protection of the 'right to privacy', recognized in Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and in many other international as well as regional human rights instruments[2] can play an important role in managing new digital threats to human rights, which are inextricably linked to the personal data that powers the engines of digitized societies.

People around the globe are witnessing remarkable progress in technological developments, that enhance quality of life and stimulate economic growth. With the benefits these technologies entail, people are also experiencing how these technologies can be used to track them. The progressive advancement of information technology, given its ability to gather, analyze, and distribute personal information, has created an immediate need for legislative measures. Additionally, advancements in areas such as medical research, telecommunications, transportation systems, and financial transfers have significantly amplified the amount of data generated by individuals. Through interconnected computers utilizing high-speed networks and advanced processing systems, comprehensive profiles of individuals can be compiled without relying on a single centralized computer system.

---

[1] Warren & Brandeis, *The 'right to privacy'*, Vol. IV, Harward Law Review (1890)

[2] Article 16 of the 'Convention on the Rights of the Child'; Article 14 of the 'International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families'; Article 22 of the 'Convention on the Rights of Persons with Disabilities'; Article 10 of the 'African Charter on the Rights and Welfare of the Child'; Article 11 of the 'American Convention on Human Rights'; and Article 8 of the 'Convention for the Protection of Human Rights and Fundamental Freedoms'.

Social media is one aspect of technology, which helps people to connect with one another virtually. The primary issue which arises with social media is the freedom which it provides to its users. The freedom is not an issue but its misuse by the users causes the problems. Social media provides its users the power to post anything on any of the social media platforms without paying heed to the consequences following it. Furthermore, it allows the governments, corporations and several other entities, unrestricted access into the lives of individuals. The concept of privacy is still budding as of now, but countries like Europe, USA, etc. have developed this concept to a great extent.

In 2017, the Supreme Court of India has recognised the concept of privacy as a fundamental right. The Supreme Court also acknowledged the absence of an elaborative privacy law and the inadequacies of existing regulations in addressing data privacy concerns and hence prompted the Indian government to formulate an exhaustive privacy legislation. Inspite of its several attempts, the privacy bill was rejected in both 2019[3] as well 2022[4] session. In its 2022 iteration, technology firms raised concerns regarding the bill's providing extensive exemptions to government entities, limitations on safeguarding user data, and constraints on data exports. The latest version was then put forward for public consultation in November 2022, during which over 20,000 stakeholder comments were received for lawmakers that were to be considered before finalization of the draft. On August 9, 2023, India enacted a data protection law that aims to regulate the processing of users' data by various entities, known as the 'Digital Personal Data Protection Act' (referred to as "the Act"). Furthermore, It lays down guidelines for organizations as to how to properly handle the personal data and grant its citizens control over their personal information.

'The Digital Personal Data Protection Act, 2023' (DPDPA) in India showcases a significant advancement in data protection efforts, yet it holds certain deficiencies regarding online privacy. One main concern centers on the susceptibility to exploitation or infringement of data privacy due to loopholes or ambiguities within the legislation. These gaps could lead to the unauthorized use of personal information, tracking of data, and the improper utilization of user data on online platforms, as a result endangering individuals' privacy.

---

[3] 'The Personal Data Protection Bill, 2019' (Bill No. 373 of 2019), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[4] 'The Digital Personal Data Protection Bill, 2022', Ministry of Electronics & Information Technology, Government of India, accessed August 9, 2023, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

Moreover, apprehensions arise from the Act's provisions regarding legitimate uses of personal data without explicit consent, commonly referred to as 'legitimate uses.'[5] The broad exemptions provided under this concept have sparked worries about potential privacy breaches and data exploitation on online platforms. The expansive nature of legitimate uses might undermine individual privacy rights and facilitate data misuse by entities handling personal information.

Additionally, questions arise concerning the Act's treatment of processing personal data available in public domain that has been provided by users, particularly regarding the level of protection afforded to such data. The Act's clauses on publicly available data and exemptions for its processing could impact user privacy on online platforms, particularly concerning data scraping and third-party use without explicit consent.

2. Research Questions

a) What are the existing privacy legislation and regulatory frameworks in India regarding online platforms?

b) What are the challenges of privacy transparency mechanisms at the different stages of digital transition?

c) How effective are the current privacy laws in ensuring transparency and safeguarding user privacy?

d) What are the potential areas of improvement for privacy laws with reference to online platforms in India?

3. Literature Review:

The literature review will provide an overview of the existing literature on transparency, privacy, and media communication in India. The review will examine the legal and ethical frameworks governing media communication, including privacy laws, media ethics, and the right to information. The review will also discuss case laws and examples related to the Indian legal frameworks regarding privacy invasion in the digital sphere.

[5] Section 7, 'The Digital Personal Data Protection Act, 2023'

a. **Heide Wunder, Considering 'Privacy' and Gender in Early Modern German-Speaking Countries (2022) In Early Modern Privacy: Sources and Approaches (pp. 63-78) available at https://www.jstor.org/stable/10.1163/j.ctv29sfvfg.9, (Last Visited on Jan 10, 2023).**

Heide Wunder's article underscores the need for privacy policies to regulate social media. The pervasive influence of these platforms blurs the distinction between public and private matters. Wunder argues that privacy concerns are heightened by the increasing sharing of personal information online. To address this, she advocates for dedicated policies that protect individuals' personal information and uphold privacy rights. Comprehensive regulations would strike a balance between the benefits and risks of social media, enabling individuals to manage control over their personal information while benefiting from the platforms' connectivity and communication features. Wunder emphasizes the urgency of implementing such regulations in light of the evolving privacy landscape.

b. **Woodrow Hartzog, "What is Privacy? That's the Wrong Question", 88 The University of Chicago Law Review 1677 (2021)**

Hartzog contends that the notion of privacy cannot be limited to a fixed definition, arguing instead for its multidimensional nature that varies across contexts and individuals. He emphasizes the need to understand privacy as a contextual concept that evolves alongside technological advancements and societal changes. Hartzog critiques existing privacy frameworks and proposes a comprehensive regulatory approach that considers power dynamics and promotes meaningful constraints on data practices, individual control, and transparency. By challenging conventional notions of privacy, Hartzog's article contributes to ongoing discussions in privacy law and policy, urging a re-evaluation of assumptions and the development of more efficient strategies for privacy protection in the digital era.

c. **Margot E. Kaminski and Jennifer M. Urban, "The Right To Contest AI", 121 Columbia Law Review Association, Inc.1957 (2021)**

Kaminski and Urban's research highlights the urgent need for the protection of privacy rights. They emphasize the growing concerns and genuine demands for data privacy, stressing the importance of safeguarding individuals' privacy. Their work calls for robust measures to address these concerns in our increasingly digital world. By raising

awareness and advocating for strong privacy protections, Kaminski and Urban contribute to the ongoing discourse on privacy. They emphasize the need to strike a balance between technological advancements and privacy preservation, urging policymakers and organizations to prioritize effective measures that adapt to the evolving privacy landscape.

d. **Sangeeta Mahapatra, "Digital Surveillance and the Threat to Civil Liberties in India Author(s): Institute of Global and Area Studies", (GIGA) (2021) available at: https://www.jstor.org/stable/resrep31794 (Last Visited on May 20, 2022).**
Sangeeta Mahapatra's research raises concerns regarding the use of new surveillance techniques and the lack of adequate privacy laws in India. She highlights privacy as one of the fundamental rights and expresses apprehension about the employment of 'digital surveillance system's without comprehensive data privacy legislation. Mahapatra also highlights the engagement of certain companies in surveillance practices, particularly during the COVID-19 pandemic when contact tracing devices were extensively used. The research underscores the need for India to adopt suitable measures and establish robust frameworks to protect privacy rights and address the ethical and legal implications associated with surveillance technologies.

e. **Young, Kaliya, et al. "Key Differences Between the U.S. Social Security System and India's Aadhaar System." The Promise of Public Interest Technology: In India and the United States, New America, 2019, 137–154. (2019).**
Y. Kaliya points out that India's Aadhaar system, similar to the U.S. Social Security Number system, lacks specific legislation for handling individual data, unlike the U.S. with its robust privacy laws. Privacy rights in India rely on judicial decisions, while the U.S. strictly regulates SSNs and imposes stringent privacy protections. The research provides an overview of Aadhaar and SSN, examining historical and present risks. It discusses the role and positioning of each number within their respective systems, legal and regulatory frameworks, operational transparency, the establishment of comprehensive databases in India, and the contrasting use of the numbers in employee enrollment and financial services.

f. **Bhandari, V. (2018). "Privacy Concerns In The Age Of Social Media", 45 India International Centre Quarterly 66–81 (2020)**

V. Bhandari points out that various entities, including government agencies and private organizations, collect personal data from individuals without their knowledge or consent. This data is stored and analyzed to reveal personal interests, past experiences, and online behavior. The rise of big data has enabled the creation of comprehensive individual profiles, granting unprecedented power to carry out surveillance and make impactful decisions. Bhandari emphasizes the pervasive nature of gathering data and the lack of transparency surrounding these activities. Through advanced data analytics, both state, as well as non-state actors, can delve deep into personal information, monitoring individuals and exerting a significant impact on their lives.

g. **Varun Kalra and Ramisba Jain, "An Armistice Between 'right to privacy' and Right to Surveillance", (2018), available at www.manupatrafast.com (Last visited on March 18, 2023).**

Varun Kalra and Ramisba Jain's paper critically examines the legal status of privacy right in India. They examine the progress of this recently recognized right via a case-by-case analysis. The paper throws light upon controversies surrounding privacy, emphasizes the need for an elaborative privacy policy, and also, evaluates the use and potential abuse of surveillance rights. Furthermore, the authors aim to provide recommendations for resolving the conflict between privacy and surveillance, while establishing clear restrictions on privacy, acknowledging surveillance agencies, and, implementing a code of conduct to prevent abuse of power. The paper addresses several unanswered questions about privacy in the Indian context, such as the impact of WhatsApp's privacy policy changes, and the extent of Aadhaar's role as a surveillance mechanism. These unresolved issues are significant in ongoing cases before the Apex Court of India.

h. **V. Bhandari & and Renuka Sane, "Towards a privacy framework for India in the age of the internet", (2017) available at http://www.nipfp.org.in/publications /working-papers/1768/ (Last visited on April 13, 2023)**

V. Bhandari and Renuka Sane highlight the significant advancements in surveillance technology and the accessibility of personal information, leading to enhanced surveillance capabilities. This raises concerns about striking a balance between the

benefits of big data and the potential threats to privacy. The existing policy landscape lacks clarity, necessitating the establishment of legal frameworks, regulations, improved privacy protections, and increased awareness of privacy rights. This comprehensive approach aims to address the challenges of extensive surveillance practices and ensure the adequate protection of individuals' privacy rights.

i. **Smith Krishna Luthra and Vasndha Bakhru, Publicity Rights and 'right to privacy', 31 National Law School of India Review (2019).**

Smith Krishna Luthra and Vasndha Bakhru's paper explores the concept of the publicity right, which involves the protection, control, and economic benefits derived from one's image, name, or likeness. The article examines the development of the publicity right alongside the 'right to privacy' in different jurisdictions, including the United States, United Kingdom, and India. While the United States recognizes the publicity right as a distinct right, the United Kingdom does not. In India, the publicity right is acknowledged within the framework of Intellectual Property Rights, but its integration with privacy rights is still in its early stages.

j. **H. Akın Ünver, "Politics of Digital Surveillance, National Security and Privacy, Centre for Economics and Foreign Policy Studies", (2018) available at https://www.jstor.org/stable/resrep17009, (Last Visited on Jan 02, 2023).**

In his article, H. Akın Ünver explains methods of digital surveillance. He highlights the effectiveness of digital surveillance in monitoring individuals' activities. One method mentioned is ICT monitoring, which involves tracking online activities through Internet Communication Technology. This form of surveillance enables authorities to monitor digital interactions. Another method discussed is remote sensing and geo-location, which utilizes GPS devices to collect data/information and track individuals' movements. In certain locations, biometric machines are used to gather data for surveillance purposes. These methods showcase the diverse techniques employed in digital surveillance to monitor along with gathering information on individuals.

k. **Myriam Dunn Cavelty and Matthias Leese, "Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity", 5 European Review of International Studies 49-69 (2018)**

Myriam Dunn Cavelty and Matthias Leese express their concerns regarding the unauthorized sharing of individuals' personal data. They emphasize the significance of personal data and argue against its transfer to third parties. The focus of this article is on the politicization of security, which differs from the concept of securitization. Politicization implies that security issues are prone to controversial public debates without predetermined outcomes regarding their management. To evaluate the empirical processes of politicization, the authors propose examining privacy as a central concept and a primary means of resistance against security logic. This approach allows for an exploration of how privacy is used as a tool to challenge and contest prevailing security narratives.

l. **Dr. Payal Jain & Ms. Kanika Arora, "Invasion of Aadhaar on 'right to privacy': Huge Concern of Issues & Challenges", 45 Indian Bar Review (2018)**

According to Gaurav Mittal and Abhishek Sharma, the Supreme Court's ruling, recognizing the privacy right as a fundamental right intertwined with the right to life and liberty, has instilled a sense of hope and optimism among LGBT communities. This landmark verdict has provided these communities with a renewed faith that they can overcome the harsh and unjust law outlined in Section 377 IPC, which criminalizes their personal and sexual lives. Furthermore, this decision establishes a future-oriented objective for governments to strive towards, emphasizing the need for guidelines and measures to support the rights of the LGBT community and facilitate progressive change. It signifies a positive step forward in paving the path for a more inclusive society and promoting equality for all individuals.

m. **Radha Devi, "Evolution of 'right to privacy' Jurisprudence-A Critique" Journal of Indian Law Institute (2018)**

In her evaluation, Radha Devi assessed the existing protective measures in India concerning the 'right to privacy' and expressed concern regarding the inadequacy of privacy laws. According to Devi, the 'right to privacy' is a multifaceted and all-encompassing concept, encompassing personal intimacies, family life, marriage, procreation, name, and sexual orientation. It implies an individual's entitlement to be

left alone, ensuring control over crucial aspects of life and representing fundamental liberty. However, the ability of both state as well as non-state actors to violate privacy has significantly increased, with unauthorized leaks, hacking, and other cybercrimes posing threats to vulnerable databases.

Devi further highlighted that modern computer systems store vast amounts of sensitive data, yet India lacks a specific law dedicated to data protection. The absence of comprehensive data protection legislation necessitates the establishment of guidelines for the collection, storage, processing, and use of data by both state and non-state actors. It is crucial to ensure that collected information/data is utilized solely for the objectives for which it was gathered. Consequently, India requires robust data laws for protection of data that address these concerns and provide a framework for safeguarding privacy rights in an increasingly digitized society.

n. **Zhi Zhou, Yue Wang, Eam Thwang Teo (2016) in his article "A Framework for Semantic People Description in Multi-camera Surveillance Systems".**

This paper presents a framework for people re-identification, an important application in surveillance systems with separate cameras. The framework utilizes soft-biometric traits as descriptors, which offer more robustness to changing factors compared to low-level features like color and texture. By extracting soft-biometric traits from different parts of the detected individuals, the framework constructs a comprehensive descriptor. People re-identification is then performed using a Nearest Neighbor matching strategy. The proposed method is evaluated on the SAIVT-SoftBio database, consisting of videos from surveillance cameras, and other image-based datasets. Comparative analysis with state-of-the-art methods demonstrates the efficacy of the suggested framework in achieving good performance. Additionally, the framework is evaluated for open ID recognition, yielding favourable results.

o. **D. Galantonu, "The Big Brother Fear: Four Perspectives on Surveillance", 33 American Intelligence Journal 59-64 (2016).**

In his article, Galantonu drew attention to the privacy concerns associated with surveillance. He pointed out that surveillance involves the observation and tracking of individuals' activities, behaviour, or personal information with the intention of influencing, controlling, directing, or promoting them. The perspective on this practice can be viewed in two contrasting ways: the positive aspect, where monitoring behavior

is aimed at safeguarding individuals, or the negative aspect, where surveillance is conducted for covert purposes like manipulating, influencing, blackmailing, or exploiting opponents.

p. **A. Tarafder, "Surveillance, Privacy, And Technology: A Comparative Critique Of The Laws Of USA And India" available at http://www.jstor.org/stable/44782800 (2015) (Last Visited May 10, 2020)**

The paper examines the laws pertaining to protection of privacy in two prominent jurisdictions: the United States of America (US) and India. Despite significant differences in socio-economic and political contexts, these countries present intriguing subjects for analysis. Their distinct demographics, geopolitical structures, and independence from communitarian regulatory mechanisms allow them to develop unique domestic legal frameworks tailored to their specific cultural needs. The paper investigates a concerning pattern that emerges from the shared positioning of these nations in terms of privacy protection: one possesses a robust, functional, and comprehensive legislative framework, while the other lacks a clear policy in this regard. Both jurisdictions seem to prioritize "national security" over individual liberties, which has become an accepted norm.

q. **Ashley S. Deeks, An International Legal Framework for Surveillance, 55 Virginia Journal of International Law, 291–368 (2015)**

This article examines three interconnected enigmas that arise from the sudden transformation of surveillance practices. Firstly, it examines the limited attention given by international law to the regulation of governments' surveillance of other states' nationals and investigates the reasons behind this gap. Secondly, drawing on international relations theory, it argues that the establishment of new international norms concerning surveillance is both probable and necessary. Thirdly, it identifies six process-oriented norms that states can and must adopt to ensure efficacious privacy safeguards in international surveillance, while also preserving their lawful national security interests. These norms, including constraints on data usage, regular reviews of surveillance authorizations, and independent oversight, aim to enhance transparency, accountability, and legitimacy in foreign surveillance activities.

r. **Acharya, Bhairav (2015): "The Four Parts of Privacy in India", Economic & Political Weekly, 50(22), 30 May 2015**

The paper examines four aspects of privacy in India that impact the growth of privacy laws. It also explores various theoretical understandings of privacy, encompassing philosophical and legal perspectives. The author analyses privacy claims involving the press, decisional autonomy, state surveillance, and personal information. However, the research does not explore the reasonable justifications for state surveillance or propose remedies for violations of the 'right to privacy'.

s. **Saha, Himaloya and Rahman, Saquib (2015): "Personal Data Protection Laws Concerning Bangladesh", IOSR Journal of Humanities and Social Science (IOSR-JHSS), Volume 20, Issue 8, Ver. II (Aug. 2015), PP 34-43**

The author explores the adverse effects that can arise from its misuse, citing examples of individuals who have suffered as a result. The need for the enactment of personal data protection laws in Bangladesh is emphasized, and a critical analysis of the existing laws in the country is presented. The article provides a comprehensive overview of laws concerning personal data protection, which fall within the realm of the 'right to privacy'. The conclusion emphasizes the pressing necessity for legislation on personal data protection to ensure adequate data security. However, the article focuses solely on data protection issues in Bangladesh and fails to address the connection between electronic communication surveillance and data protection within the context of the 'right to privacy'.

t. **Garg, Priyam (2015): "Law On Phone-tapping In India", Academike - Lawctopus, February 4, 2015**

The author explores the various methods employed by governments worldwide to ensure national security. The emphasis lies on the need to lay down a legal framework in India that defines the permissible scope and purpose of phone tapping. Recent controversies have been discussed, and evaluations have been done comparing them to legal frameworks in international jurisdictions. However, the article primarily centers on the specific technology of phone tapping, without providing a comprehensive understanding of its historical use and modern advancements in interception methods. Furthermore, the article fails to address the use of alternative intrusion technologies for the purpose of national security.

u. **Mohanty, Bedavyasa (2014): "The Constitutionality of Indian Surveillance law: Public Emergency as a Condition Precedent for Intercepting Communication", Journal of Politics & Governance, Vol. 2, No. 4, December 2014**

The author thoroughly examined the complexities associated with intercepting communication within the legal framework of the Indian Post Office Act and the Indian Telegraph Act. The study also delved into the constitutional implications of administrative powers regarding communication interception and explored the origins and development of surveillance law in India. However, the author's analysis was limited to the Indian Post Office Act and the Indian Telegraph Act, without addressing the effectiveness of interception laws and data protection measures in meeting contemporary demands and challenges.

v. **Singh, Aniruddh (2014): "Interception of Communication", Journal of Politics & Governance, Vol. 2, No. 4, December 2014**

The author examines various procedural elements associated with communication interception and its necessity in India. The focus of the paper is on the availability, validity, and authenticity of evidence obtained through interception. The research highlights procedural aspects but overlooks the discussion on the significance of establishing consistent substantive laws to safeguard the 'right to privacy' and ensure data protection.

w. **Gautam Bhatia, "State Surveillance And The 'right to privacy' In India: A Constitutional Biography", 26 National Law School of India Review 127-158 (2014)**

The essay provides a detailed and chronological account of the Indian Supreme Court's involvement in the recognition of the 'right to privacy'. While the progress towards enacting a privacy law has stagnated and remains unresolved, the court has actively engaged with privacy issues for nearly half a century. The paper examines the constitutional aspect of the 'right to privacy', tracing its evolution, interpretation, and implementation by the judiciary. This comprehensive understanding serves as a crucial foundation for undertaking a legal and constitutional evaluation of extensive state surveillance in India. Gautam Bhatia highlights that, although the Indian Constitution does not explicitly mentions privacy, the Supreme Court of India has interpreted Article

21 in a manner similar to how the Fourth Amendment of the United States Constitution safeguards against unreasonable searches and seizures.

4. Research Gap

a) 'The Digital Personal Data Protection Act of 2023' lacks comprehensive provisions that specifically tackle the distinct privacy challenges presented by social media platforms, thereby creating potential opportunities for privacy breaches within this sphere.

b) The Act's notion of "legitimate uses" permits data processing without explicit consent under certain circumstances, which might result in data exploitation and privacy violations if not carefully regulated.

c) The Act's approach to processing publicly available data and the exemptions granted for such data raise apprehensions regarding the safeguarding of user privacy, particularly regarding data scraping and third-party utilization without explicit consent.

d) Although the Act enforces fines for failure to comply, doubts may arise regarding the efficacy of these penalties in discouraging privacy infringements on online platforms, thereby potentially exposing users to data misuse.

5. Research Objectives:

The research aims to achieve the following objectives:

a) To analyze the efficacy of the provisions of The Digital Personal Data Protection Act of 2023 concerning privacy challenges presented by social media platforms existing privacy laws and regulations related to social media platforms in India.

b) To examine the consequences of the "legitimate uses" clause in the Act regarding data processing without explicit consent in particular scenarios, with an emphasis on identifying potential hazards related to data exploitation and breaches of privacy.

c) To analyse the consequences of the Act's approach to managing publicly accessible data and the exemptions granted for such data, with a particular focus on the preservation of user privacy, particularly concerning instances of data scraping and third-party usage without explicit consent.

d) To explore the effectiveness of the fines imposed by the Act for non-compliance and to address doubts concerning their ability to deter privacy violations on online platforms, with a view to understanding the potential risks of data misuse that users may face as a result.

6. Research Hypothesis:

- The absence of specific measures outlined in the ‘Digital Personal Data Protection Act of 2023’ to confront the distinct privacy challenges presented by several social media platforms raises the probability of privacy breaches occurring within this realm.
- The incorporation of the "legitimate uses" principle in the Act permits data processing without explicit consent in certain circumstances, potentially resulting in occurrences of data exploitation and privacy violations if not closely monitored.
- The Act's approach to managing publicly available data and the exceptions it grants raise worries about safeguarding user privacy, particularly regarding data scraping and third-party usage without explicit consent, indicating a potential threat of privacy breaches in this area.
- Although the Act imposes fines for failure to comply, there are concerns about how effective these penalties are in preventing privacy violations on online platforms, indicating that users could still be at risk of data misuse.

7. Research Methodology:

The research methodology will include a qualitative research design with a case study approach. The study will use primary and secondary sources to collect data, including legal documents, media reports, and academic literature. Data analysis will involve thematic analysis.

8. Scope and Limitations of the Study:

The study will comprehensively analyze the legal frameworks governing privacy in the digital realm within the context of India, focusing particularly on online platforms. It will explore various aspects including data protection laws, regulations, and judicial precedents. Additionally, the study will delve into ethical considerations surrounding privacy invasion on online platforms, examining issues such as data exploitation, surveillance, and user consent.

However, the study may face limitations in covering all aspects of privacy invasion within the digital sphere due to time constraints. Findings from the study may not be directly generalizable to other jurisdictions or countries with different legal frameworks and cultural contexts.

9. Tentative Chapterisation:

The proposed chapterisation of the study is as follows:

Chapter 1: Introduction

1.1 Background
1.2 Statement of Problem
1.3 Purpose of Study and Research Questions
1.4 Scope of Study
1.5 Methodology
1.6 Conclusion

Chapter 2: Historical Evolution of the 'right to privacy'

2.1 History
- 2.1.1 Informational Privacy
- 2.1.2 The Constitutional 'right to privacy'
- 2.1.3 Reductionism vs. Coherentism

2.2 Critiques of Privacy
- 2.2.1 Thomson's Reductionism
- 2.2.2 Posner's Economic Critique
- 2.2.3 Bork's View
- 2.2.4 The Feminist Critique of Privacy

2.3 Views on the Meaning and Value of Privacy
- 2.3.1 Privacy and Control over Information
- 2.3.2 Privacy and Human Dignity
- 2.3.3 Privacy and Intimacy
- 2.3.4 Privacy and Social Relationships
- 2.3.5 Privacy and Restricted Access
- 2.3.6 The Scope of Privacy
- 2.3.7 Is Privacy Relative?

2.4 Privacy and Technology
- 2.4.1 The Social dimension of Privacy
- 2.4.2 Privacy and Conflicts with Other Values

2.5 Conclusion

Chapter 3: Statutory protection to 'right to privacy'

A. Protection Under Indian Laws

3.1 Privacy under Law of Torts
- 3.1.1 Privacy Torts under Indian Law
- 3.1.2 Privacy and Defamation
  - i Meaning of Defamation
  - ii Distinguishing Defamation from other Concepts
  - iii Press and Libel Laws

iv Defamation under Indian Law of Torts
v Defamation under Common Law
- Newspaper Libel
- Slander
- Defences
- Remedy for Defamation

3.1.3 Breach of Confidentiality and Privacy
3.1.4 'right to privacy' as a Customary Right
3.1.5 Intentional Infliction of Emotional Distress
3.1.6 Privacy and Nuisance

3.2 Protection of Privacy under Criminal Law
3.2.1 Criminal Libel/Defamation
3.2.2 Right to Private Defence and Privacy
3.2.3 Sexual Offences and Privacy
- Rape
- Sexual Harassment
- Trafficking
- Statutory and Procedural safeguards to Victim of Sexual Offences
- Indecent Representation and Privacy
- Indecent Representation of Women (Prohibition) Act 1986

3.2.4 Arrest and Detention and Privacy
3.2.5 Search and Seizure and Privacy Protection
3.2.6 Consequences of non-compliance with the provision relating to searches
3.2.7 Cyber Breach of Privacy
- 3.2.7.1 Cyber Obscenity
- 'right to privacy' and Information Technology Law
- Industry Initiative
- Extra Territorial Application

3.3 Intellectual Property Rights and Privacy
3.4 Privacy under Contract Law
3.5 'right to privacy' and Privileged Communication
3.6 Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act 2016
3.7 'Data Privacy' Under The Information Technology Act, 2000 and Information Technology Rules
3.8 The Information Technology Act, 2000
3.9 Information Technology Rules, 2011
3.10 Justice B.N. Srikrishna Report 2018
3.11 The Personal Data Protection Bill, 2019
3.12 Digital Personal Data Protection Act, 2023
3.13 The Right To Information Act, 2005

B. Protection Under USA Laws

3.14 The Privacy Act, 1974
3.15 Electronic Communications Privacy Act,1986 (ECPA 1986)
3.16 Children's Online Privacy Protection Act, 2000 (COPPA 2000)
3.17 Video Privacy Protection Act (VPPA)
3.18 Sarbanes Oxley Act (SOX)
3.19 Gramm -Leach Billy Act (GLBA)
3.20 USA Patriot Act
3.21 Organisations Related to Data Protection Laws In USA

C. Protection Under European Laws

3.22 The General Data Protection Regulation (GDPR)

Chapter 4: Role of Media vis-à-vis 'right to privacy' in India

4.1 Meaning of Media
4.2 Meaning of the Press
4.3 Meaning of a Newspaper
4.4 Importance of Freedom of Press
- 4.4.1 Justifications for Freedom of Press
  - (a) Printed matter records the ideas in a permanent form
  - (b) Newspaper or book has a larger circulation than spoken words
  - (c) Freedom of the Press is nothing but the freedom of expression of every citizen
  - (d) Press recognized as an institutional limb of modern democracy
  - (e) Freedom of discussion is essential to enlighten public opinion
  - (f) Freedom to discuss public issues
  - (g) Freedom of press and free and fair elections
  - (h) Ultimate good in a free society can be reached only by a discovery of truth
  - (i) Free Trade in Ideas
  - (j) Public criticism is essential to the working of democracy
- 4.4.2 Contents of Freedom of the Press
- 4.4.3 Need for Limitation on Freedom of Press

4.5 'right to privacy' and Media
- 4.5.1 Privacy vis-à-vis Media Freedom under Common Law
  - Intrusion
  - Eavesdropping
  - False light
  - Celebrities' Right to Likeliness
- 4.5.2 Public Records are not covered under Privacy Protection
  - New York Times Rule

4.5.3 Indian Law on Libel
- Rules in Auto Shankar Case

4.6 Media Trial and Liberty of Individuals
4.7.1 Media Trial and Administration of Justice
4.7.2 Judicial Response to Media Trial
4.7.3 Contempt of Court Act, 1971
4.7 Mumbai Terror Attack Case and Freedom of Media
4.8 Sting Operation: The New Facet of Journalism
4.9.1 Threats to Privacy by Sting Operations
4.9.2 The Ethics of the Sting Operation
4.9 Regulation of Freedom of Press
4.10.1 Reasonable Restrictions on freedom of Press
4.10.2 Press Council of India
4.10.3 Norms of Journalistic Conduct
- 'right to privacy'
- Caution against Identification
- Privacy of Public Figures
- Recording Interviews and Phone Conversation
- Newspaper to Eschew Suggestive Guilt

4.10.4 Code of Ethics and Broadcasting Standards
1.11 Conclusion

Chapter 5: Legal concerns and issues regarding the protection of privacy rights

5.1 Introduction
5.2 Social Networking Platforms
5.3 Issues and Challenges in reference to protecting privacy on Social Networking Platforms
5.3.1 Information Technology Act, 2000
5.3.2 Informational Technology Rules, 2021
5.3.3 Digital Personal Data Protection Bill, 2022
5.4 Conclusion

Chapter 6: Conclusion and Suggestions

10. Proposed Month-wise plan of work and targets to be achieved:

S.No.	Proposed Work	Tentative Date
1.	Thesis Proposal Defense	October, 2023
2.	Extended Literature Review	November, 2023
3.	Identify Stakeholders and collect Empirical Data	December, 2023
4.	Approval of Title	May, 2024
4.	Progress Seminar	October, 2024
5.	Progress Seminar	Mar, 2025
6.	Pre Ph.D. Seminar	September 2025
7.	Thesis Submission	December, 2025

11. Bibliography:

The references will include a list of all the sources cited in the proposal, including legal documents, academic literature, media reports, and online sources. The references will follow the citation style recommended by the research supervisor.

- Professor S.R., Bhansali, Constitutional Law of India, 465 (Universal Law Publishing Company Pvt. Ltd., Delhi 2nd ed. 2014)
- Rutvi Zamre, From streets to tweets: Surveying the impact of online activism, ORF (Sept. 8, 2020), https://www.orfonline.org/expert-speak/streets-tweets-surveying-impact-online-activism/ .(Last visited 21 April, 2023)
- Shoaib Daniyal, Why is the Indian Government at War with Twitter, Scroll.in (Jul. 8, 2021),https://scroll.in/article/999171/why-is-the-government-of-india-at-war-with-twitter (Last visited 18 March, 2023)
- Chandrima Banerjee, How social media gets away with spreading lies, Times of India (May 5, 2022), https://timesofindia.indiatimes.com/india/how-social-media-is-getting-away-withdisinformation/articleshow/91318044.cms (Last visited on 12 March, 2023)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R.139(E), 2(1) (w).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E)
- Maya Mirchandani, Digital hatred, real violence: Majoritarian radicalisation and social media in India, ORF (2018), https://www.orfonline.org/wp-content/uploads/2018/08/ORF_OccasionalPaper_167_DigitalHatred.pdf, (last visited Oct. 30, 2022).
- Jack Balkin, How to Regulate (And Not Regulate) Social Media, 1 Journal of Free Speech Law 71 (2021).
- Sarah Myers West, Raging Against the Machine: Network Gatekeeping and Collective Action on Social Media Platforms, 5(3) Media and Communication 28, 28 (2017).
- Rebecca Mackinnon, Consent Of The Networked: The Worldwide Struggle For Internet Freedom (New York, Basic Books, 2012).
- Kai Reimer and Sandra Peter, Algorithmic audiencing: Why We Need to Rethink Free Speech on Social Media, 00(0) Journal of Information Technology 1 (2021).
- Amber Sinha, The Networked Public, How Social Media Is Changing Democracy, 174 (Rupa Publications, 2019)

- Pritika Rai Advani, Intermediary Liability in India, EPW (Dec 14, 2013), https://www.jstor.org/stable/24479053 .
- Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, Centre for Internet and Society, (Apr. 27, 2012), https://cis-india.org/internet-governance/chilling-effects-on-freeexpression-on-internet
- Torsha Sarkar & Gurshabad Grover, Content Takedown and Users Rights, Centre for Internet and Society (Feb 14, 2020), https://cis-india.org/internet-governance/blog/content-takedown-and-users-rights-1 .
- Daniyal, supra note 6; Soumyarendra Barik, Facebook may Proactively Censor Content to protect Itself from Legal or Regulatory Actions, Medianama (Sept 2, 2020), https://www.medianama.com/2020/09/223-facebookcensor- content-avoid-legal-regulatory-challenge/.
- Madhavi Goradia Divan, Facets of Media Law, 7 (2nd Ed. Eastern Book Company, 2018).

DrillBit

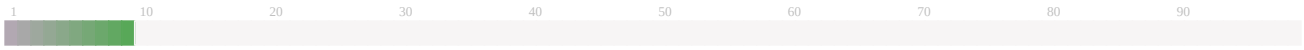
The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

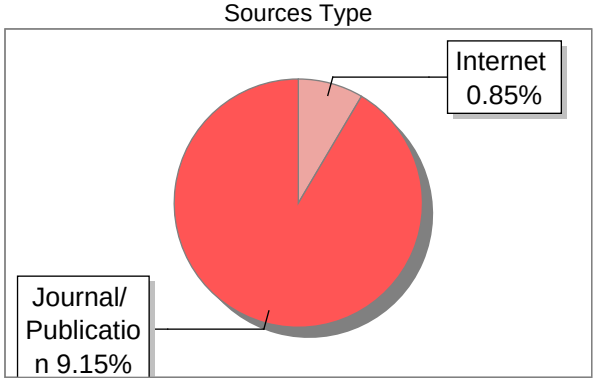
Author Name	Anushmi Jain
Title	PRIVACY INVASION IN THE DIGITAL SPHERE
Paper/Submission ID	1838288
Submitted by	research@iudehradun.edu.in
Submission Date	2024-05-20 12:52:44
Total Pages, Total Words	24, 6379
Document type	Synopsis

Result Information

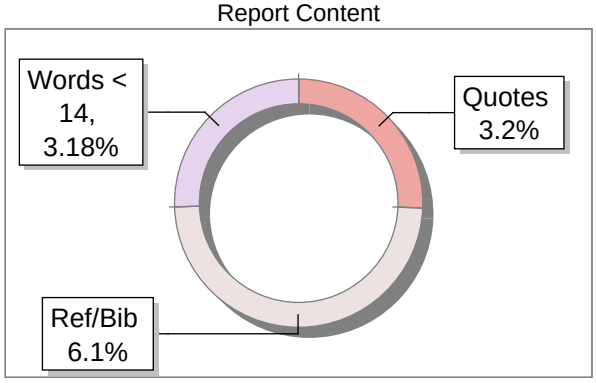
Similarity **10 %**



Sources Type



Report Content



Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Source: Excluded < 14 Words	Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File